UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,855	03/19/2004	Lauri Paatero	915-008.021	7421

4955 7590 04/21/2008

WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
04/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,855	PAATERO, LAURI	
	Examiner	Art Unit	
	ANDREW L. NALVEN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-19 and 21-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-19, 21-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 are pending.

Response to Arguments

2. Applicant argues on page 16 that one of ordinary skill in the art would not have been motivated to combine Rindsberg and Herbert. Examiner respectfully disagrees.

3. Applicant asserts that in combining Herbert's repeated generation of keys one would use the repeated generation to modify Rindsberg's shared keys. Examiner respectfully disagrees. Examiner has combined Rindsberg and Herbert in order to modify Ridnsberg's unique key that is used to re-encrypt the received patch program. Rindsberg re-encrypts the received patch after verification (Rindsberg, column 8 lines 23-33) and stores it to memory at a host (Rindsberg, column 8 lines 23-33, transfers to host and stored). One of ordinary skill in the art would recognize that using different keys increases security. Using only a single key means that if that key is compromised, all data encrypted using the key is compromised. Herbert teaches just such an improvement by disclosing that pages are encrypted before being sent for storage or verification using keys generated by a random number generator (Herbert, column 3 lines 1-15). Hence, one of ordinary skill in the art would recognize that Herbert's repeated key generation offers the advantage of increasing the strength of the encryption by using multiple keys with smaller data samples (Herbert, column 4 lines

40-46). Further, contrary to Applicant's arguments, the modification of Rindsberg would not change the principle operation of Rindsberg's invention. Rindsberg's invention operates by using a unique key that is known only to the device to re-encrypt received data. The unique key feature is not a portion of the principle operation of the device. The principle operation of the device is that a key known only to the device is used to re-encrypt. Changing the unique key known only to the device to a rotating key known only to the device does not change the principle operation of the device. The device would operate in the same manner: receiving data encrypted with a shared key, decrypting the received data with the shared key, and re-encrypting the data with a key known only to the device.

4. Applicant's remaining arguments filed 2/25/2008 have been fully considered but they are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7, 9-11, 17-21, 23, 25-26, 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rindsberg US Patent No. 6,970,565 in view of Herbert et al US Patent No. 7,149,901 and Enichen et al US Patent No. 6,333,983.

6. With regards to claims 1, 17, 31-36, Rindsberg teaches a method of enhancing data security, comprising reading encrypted data external to a secure execution environment of an electronic device to which access is restricted, wherein said encrypted data comprises program code to be executed in said electronic device, (Rindsberg, column 6 lines 20-28) the method comprising the steps of verifying, in said secure execution environment, the integrity of data of said encrypted data to be written into storage wherein said data is to be executed in the electronic device (Rindsberg, column 8 lines 19-33, if integrity of patch passes), and encrypting, in said secure execution environment (Rindsberg, column 8 lines 19-33, encrypting using the unique key) the data by means of said secret key (Rindsberg, column 8 lines 19-33, encrypting using the unique key) and writing the encrypted data into storage wherein at least some of said storage is external to said secure execution environment (Rindsberg, column 8 lines 19-33, encrypted patch stored in memory, Figure 2 Item 78). Rindsberg fails to specifically teach the generating of keys repeatedly and the use of strong and weak encryption. However, Herbert teaches generating, in a secure execution environment of an electronic device to which access is restricted, a new secret key repeatedly and using the new secret key for encryption of files to be stored (Herbert, column 3 lines 1-15, random number generator generates new encryption keys for storing encrypted pages in secure environment). Further, Enichen teaches the receiving of strongly encrypted data, decrypting that data, and re-encrypting using less strong encryption (Enichen, column 12 lines 14-24, converts encryption from RK to weak key W). At the time the invention was made, it would have been obvious to a person of ordinary skill in

the art to utilize Herbert's key generation method and Enichen's encryption method with Rindsberg's secure downloading system because it offers the advantage of increasing the strength of the encryption by using multiple keys with smaller data samples (Herbert, column 4 lines 40-46) and allowing for a faster decryption process due to the weaker key strength and allows for meeting export restrictions (Enichen, column 1 lines 25-45).

7. With regards to claims 2, 18, Rindsberg as modified teaches a new secret key is generated when the device is booted (Herbert, column 4 lines 20-30, random number generator continually generates keying material).

8. With regards to claims 3, 19, Rindsberg as modified teaches a new secret key is generated repeatedly during runtime (Herbert, column 3 lines 1-15, generated for new pages).

9. With regards to claims 4, 20, Rindsberg as modified teaches the data comprises program code (Rindsberg, column 7 lines 23-25, patch program).

10. With regards to claims 5, 21, Rindsberg as modified teaches storage comprising temporary memory (Rindsberg, column 7 lines 41-44, RAM).

11. With regards to claims 7, 23, Rindsberg as modified teaches authenticating, in said secure execution environment, the program code to be written into storage to ensure that the program code originates from a trusted program code provider (Rindsberg, column 8 lines 12-19, authenticates that patch came from intended source and was received without error).

12. With regards to claim 9, Rindsberg as modified teaches the step of generating a new secret key includes the step of generating a plurality of new secret keys wherein each new secret key is used to encrypt a respective subset of the data (Herbert, column 4 lines 20-30, random number generator continually generates keying material, column 4 lines 40-46).

13. With regards to claims 10, 25, Rindsberg as modified teaches calculating, in said secure execution environment, integrity data for data to be stored in said storage (Herbert, column 3 lines 10-16) and storing the calculated integrity data (Herbert, column 3 lines 10-16).

14. With regards to claims 11, 26, Rinsbert as modified teaches the integrity data comprising a message authentication code (Herbert, column 3 lines 10-16, hash).

15. Claims 6 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rindsberg US Patent No. 6,970,565, Enichen et al US Patent No. 6,333,983 and Herbert et al US Patent No. 7,149,901 as applied to claim 1 above, and further in view of Hoskinson US Patent No. 5,455,862.

16. With regards to claims 6, 22, Rindsberg as modified fails to teach reordering address locations of said storage in address space at the time of boot, wherein the order of the address locations in address space is altered. However, Hoskinson teaches reordering address locations of said storage in address space at the time of boot, wherein the order of the address locations in address space is altered (Hoskinson, column 7 lines 13-37, at initial loading or program code all logical address are modified).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Hoskinson's address encryption method with Rindsberg as modified because it offers the advantage of preventing an observer from attempting to tap into the circuitry to discover the program and code and other data stored in the memory (Hoskinson, column 7 lines 31-37).

17. Claims 8 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rindsberg US Patent No. 6,970,565, Enichen et al US Patent No. 6,333,983 and Herbert et al US Patent No. 7,149,901 as applied to claim 1 above, and further in view of Best US Patent No. 4,278,837.

18. With regards to claims 8 and 24, Rindsberg as modified fails to teach combining the address of the location in said storage, to which location the encrypted data is to be written, with the new secret key and using the combination of the address and the new secret key to encrypt said data wherein the encrypted data becomes associated with the address. However, Best teaches combining the address of the location in said storage, to which location the encrypted data is to be written, with the new secret key (Best, column 14 lines 31-45, uses random number and address) and using the combination of the address and the new secret key to encrypt said data wherein the encrypted data becomes associated with the address (Best, column 14 lines 31-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Best's method of encryption with Rindsberg as modified because it offers the advantage of helping keep program code secure at all times and remove the

need to have unenciphered code ever be used or stored outside the processor environment (Best, column 3 lines 1-20).

19. Claims 12-14, 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rindsberg US Patent No. 6,970,565, Enichen et al US Patent No. 6,333,983, and Herbert et al US Patent No. 7,149,901 as applied to claim 11 above, and further in view of Cassagnol et al US Patent No. 6,438,666.

20. With regards to claims 12, 27, Rindsberg as modified teaches generated keys as noted above, but fails to teach the message authentication code being calculated using a secret key. However, Cassagnol teaches a message authentication code being calculated by using a secret key (Cassagnol, column 7 lines 39-62). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Cassagnol's method of computing message authentication codes with Rindsberg as modified because it offers the advantage of helping ensure that all ensuring that a processor only runs valid and authenticated programs (Cassagnol, column 7 lines 39-62).

21. With regards to claim 13, Rindsberg as modified teaches different message authentication codes being calculated for different parts of the data by means of different new secret keys (Cassagnol, column 7 lines 39-62, Herbert, column 4 lines 20-30).

22. With regards to claims 14, 28, Rindsberg as modified teaches verifying in said secure execution environment the correctness of the message authentication code that

is associated with the read data and stopping device operation if said message authentication code is different (Cassagnol, column 7 lines 39-62, only allows process to decrypt if MAC is verified).

23. Claims 15-16, 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rindsberg US Patent No. 6,970,565, Enichen et al US Patent No. 6,333,983 and Herbert et al US Patent No. 7,149,901 as applied to claim 11 above, and further in view of Christie et al US Patent No. 7,130,951.

24. With regards to claims 15, 29 Rindsberg as modified fails to teach setting a process arranged in the electronic device in one of at least two different operating modes and storing protected data relating to the device security in at least one storage area of the a storage circuitry wherein the process is given access to said storage area in which said protected data is located when a secure processor operating mode is set and the processor is denied access to said storage area when a normal processor operating mode is set. However, Christie teaches setting a process arranged in the electronic device in one of at least two different operating modes and storing protected data relating to the device security in at least one storage area of the a storage circuitry (Christie, column 4 lines 25-51) wherein the process is given access to said storage area in which said protected data is located when a secure processor operating mode is set and the processor is denied access to said storage area when a normal processor operating mode is set (Christie, column 5 lines 30-51, denied access to trusted memory areas, column 3 lines 55-63). At the time the invention was made, it would have been

obvious to a person of ordinary skill in the art to utilize Christie's method of processor modes because it offers the advantage of decreasing the likelihood of applications interfering with each other (Christie, column 1 lines 32-50).

25. With regards to claims 16, 30, Rindsberg as modified teaches the setting of processor modes is performed by protected applications (Rindsberg, column 9 lines 10-20).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Primary Examiner, Art Unit 2134